



Watchlist Internet

Internet-Betrug, Fallen und Fakes im Blick

BETRUG IM INTERNET

So schützen Sie sich

◀ www.watchlist-internet.at

Die Broschüre orientiert sich
an den Regeln Einfacher Sprache.



Einkaufen im Internet

Die Gefahren

Einkaufen im Internet ist beliebt: Man kann jederzeit und bequem von zu Hause aus shoppen.

Leider gibt es beim Online-Einkaufen auch Gefahren: Betrüger:innen gaukeln Ihnen vor, billige Produkte im Internet zu verkaufen.

Solche Fake-Shops sehen oft gut gemacht aus. Einkaufen sollten Sie dort aber nicht. Denn: Sie verlieren Ihr Geld. Sie bekommen keine Ware oder etwas ganz anderes als Sie bestellt haben.

So schützen Sie sich

Impressum überprüfen. Bevor Sie auf einer unbekanntem Internetseite einkaufen, suchen Sie nach einem Impressum. Dort muss stehen, welchem Unternehmen die Webseite gehört. Kaufen Sie nicht ein, wenn es kein Impressum gibt!

Suchmaschine (zum Beispiel Google oder Bing) fragen. Geben Sie den Namen des Shops und Wörter wie „Erfahrungen“ oder „Betrug“ in die Suchmaschine ein. Oft finden Sie so Warnungen. Gibt es weder positive noch negative Ergebnisse, lassen Sie lieber die Finger von diesem Shop.

Preise vergleichen. Vergleichen Sie die Preise auf Seiten wie geizhals.at oder idealo.at. Sind die Produkte dort viel teurer als auf der Website, spricht das für Betrug.

Betrügerische Nachrichten

Die Gefahren

Mit betrügerischen E-Mails, sogenannten Phishing-Nachrichten, versuchen Kriminelle Daten zu stehlen. Betrüger:innen versenden dafür E-Mails im Namen bekannter Unternehmen oder von Banken. Sie sollen auf einen Link klicken, der zum Beispiel auf eine gefälschte Login-Seite einer Bank führt. Dort sollen Sie persönliche Daten eingeben, die in den Händen Krimineller landen.

Für diese Masche werden auch SMS („Smishing“) oder Telefonanrufe („Vishing“) verwendet.

So schützen Sie sich

Melden Sie sich wie gewohnt an. Klicken Sie bei Nachrichten von Banken oder Unternehmen, bei denen Sie Kund:in sind, nicht auf Links in E-Mails oder SMS. Wechseln Sie in den Browser und loggen Sie sich in Ihr Benutzerkonto ein. Überprüfen Sie dort, ob es die Nachricht gibt.

Absender:in überprüfen. Kriminelle geben sich meist als bekanntes Unternehmen aus. Kontrollieren Sie, wer Ihnen eine Nachricht sendet. Stimmen Name der Absender:innen und die E-Mail-Adresse tatsächlich überein?

Keine vertraulichen Daten preisgeben. Sie werden aufgefordert, ein Passwort oder ähnlich vertrauliche Daten zu übermitteln? Machen Sie das niemals über E-Mail, SMS oder telefonisch.

Gefährliche Programme

Die Gefahren

Mit Schadsoftware versuchen Kriminelle Zugang zu Netzwerken, Computern, Tablets oder Mobilgeräten zu bekommen.

Diese Geräte oder Systeme sollen geschädigt werden, um zum Beispiel an Geld oder Daten zu kommen.

Schadsoftware kann auf vielen verschiedenen Wegen in Ihr Gerät gelangen: Kriminelle schicken Ihnen zum Beispiel gefährliche Dateien per E-Mail. Häufig versteckt sich Schadsoftware in Programmen und Apps, die eigentlich als sicher gelten.

So schützen Sie sich

Updates durchführen. Halten Sie Ihr Betriebssystem und Programme am Computer und am Smartphone auf dem aktuellen Stand. Das bedeutet: Updates sofort durchführen!

Keine Anhänge von Unbekannten öffnen. E-Mail-Anhänge sollten Sie nur von Absender:innen öffnen, denen Sie vertrauen. Sie kennen die Absenderin oder den Absender? Überlegen Sie trotzdem kurz, ob der Inhalt der E-Mail Sinn ergibt! Das gilt auch für das Anklicken von Links.

Programme aus offiziellen Stores installieren. Installieren Sie Apps und Programme nur von Stores wie „Google Play Store“ oder „App Store“.

Vorschuss- betrug

Die Gefahren

Beim Vorschussbetrug werden Sie mit einem Gewinn, einer Erbschaft oder mit günstigen Kreditangeboten geködert. Auch Erpressungsmails, vorgetäuschte Liebesbeziehungen und Notlagen sind gängige Maschen. Das Ziel: Sie sollen Geld bezahlen.

Kriminelle erfinden dabei verschiedene Gründe: Sie müssen zum Beispiel Gebühren bezahlen, bevor Sie die versprochenen Gewinne erhalten. Gutgläubigen Opfern wird so Geld abgeknöpft. Die Kriminellen machen sich anschließend aus dem Staub.

So schützen Sie sich

Keine Vorauszahlungen an Unbekannte leisten. Eigentlich sollten Sie Geld bekommen, aber plötzlich werden Zahlungen oder persönliche Dokumente von Ihnen verlangt? Das ist ein Alarmsignal.

Inhalt der Nachricht hinterfragen. Ihnen wird per E-Mail oder in einer Chat-Nachricht ungewöhnlich viel Geld versprochen? Überlegen Sie, ob das überhaupt sein kann. Kriminelle verschicken solche Nachrichten willkürlich an viele Personen.

Nach den Nachrichten suchen. Geben Sie den Text der Nachrichten oder die Namen neuer Internet-Bekanntschäften mit dem Zusatz „Scam“ oder „Betrug“ in eine Suchmaschine ein. Vielleicht stoßen Sie so auf Warnungen.

Unseriöse Investmentplattformen

Die Gefahren

Sie möchten Ihr Geld gewinnbringend anlegen? Das sollten Sie mit Vorsicht machen. Suchen Sie nach Anlage-Möglichkeiten im Internet, könnten Sie auf betrügerische Investmentplattformen stoßen.

Kriminelle versprechen dabei hohe Gewinne - ohne Risiko.

Vorkenntnisse benötigen Sie keine, stattdessen beraten Sie die Kriminellen persönlich. Klingt gut, ist aber Betrug!

So schützen Sie sich

Versprechen hinterfragen. Betrügerische Plattformen locken mit unrealistischen Angeboten. Investieren Sie nicht, wenn hohe Gewinne bei kleinen Investments versprochen werden.

Webseite überprüfen. Suchen Sie das Impressum. Gibt es keines, Finger weg! Es gibt ein Impressum? Geben Sie die Adresse der Internetseite und Worte wie „Problem“ oder „Betrug“ in eine Suchmaschine ein.

Nicht von Werbung täuschen lassen. Sie haben über eine Werbung oder in einem Online-Zeitungsartikel von der Plattform erfahren? Betrügerische Plattformen schalten viel Werbung. Werden „hohe Gewinne in kurzer Zeit“ oder „Risikofreiheit“ versprochen, ist es Betrug.

Das Internet bietet viele Vorteile und macht das Leben einfacher. Es gibt aber auch Gefahren, die Sie kennen sollten. Mit diesem Heft helfen wir Ihnen, das Internet sicher zu nutzen:

- Welche Betrugsmaschinen kommen häufig im Internet vor?
- Wie erkennen Sie diese Gefahren?
- Wie schützen Sie sich vor Internetbetrug?

Diese Broschüre wurde finanziert mit Mitteln der BAWAG Group.

Impressum

ÖIAT | Ungargasse 64, 1030 Wien

www.watchlist-internet.at


kontakt@watchlist-internet.at




Die Watchlist Internet wird unterstützt durch:



 Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

 Bundesministerium
Inneres

 Bundesministerium
Finanzen

